RSAC 2025 Conference

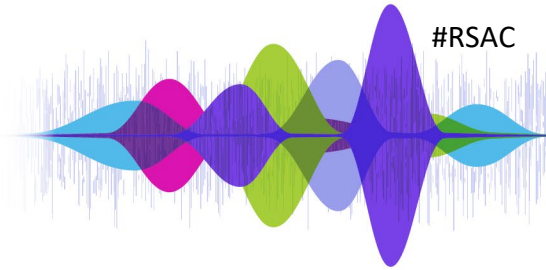
Many Voices.
One Community.

SESSION ID: FRP-R05

Deepfake vs KYC: War among AI Models, Providers, and Criminals

Philippe Lin

Senior Threat Researcher
Trend Micro



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

A famous deepfake meme at Reddit r/StableDiffusion

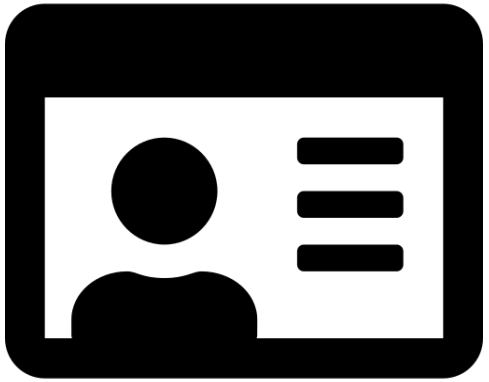
Team

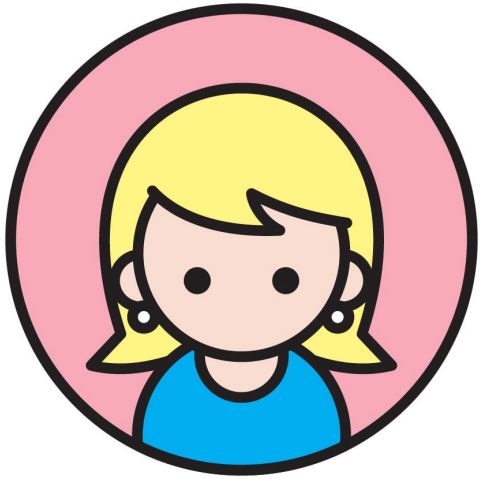
Roel Reyes

Fernando Mercês

Ryan Flores

Electronic Know-Your-Customer (eKYC)





- Identity
- Suitability
- Risks

- Anti-Money Laundering
- Counter Terrorism Financing
- Faster customer onboarding

Font Awesome Free 5.2.0 by @fontawesome - https://fontawesome.com, CC BY 4.0, via Wikimedia Commons

Image by Vectorportal.com, CC-BY-4.0

eKYC & Document scan customers

Some brand names listed here might use document scanning services and not eKYC.

infatica.io
Global Peer-to-Business Proxy Network

eKYC providers

MICROBLINK

jumio

ENTRUST
SECURING A WORLD IN MOTION

IDScan.net

acuant

persona

Shufti

GBG IDology

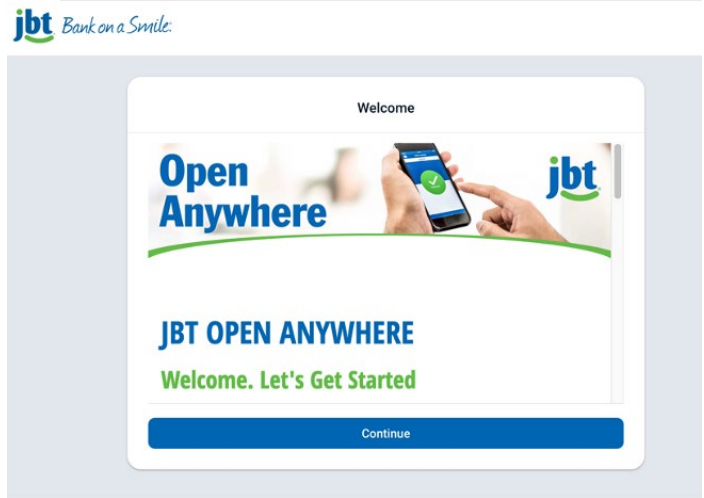
incode

veriff

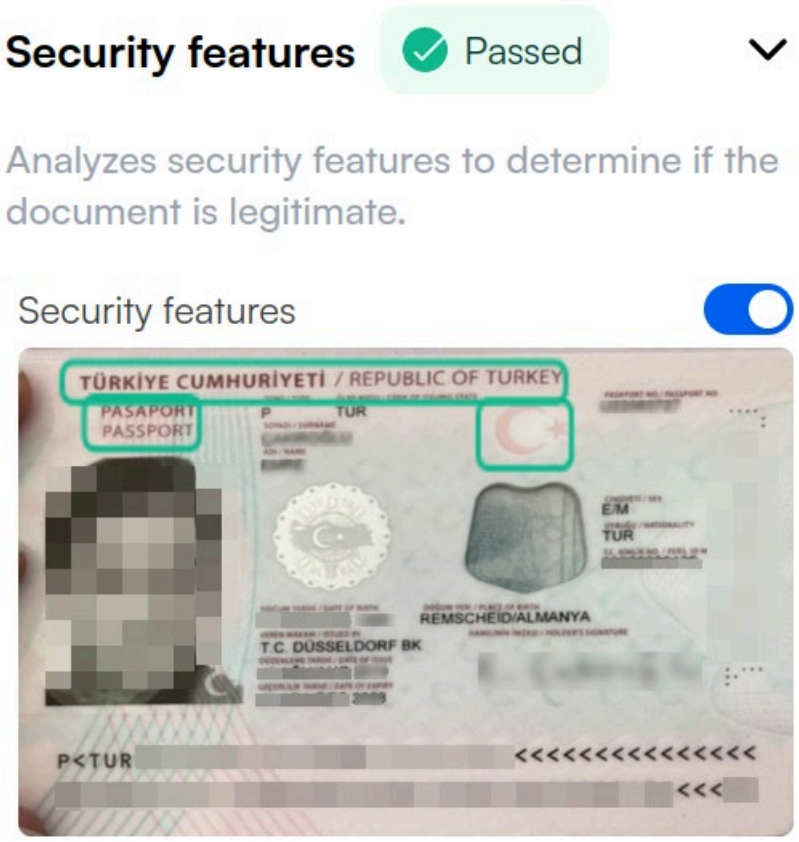
AUTOTIX

onfido
an Entrust Company

sumsub



How eKYC works?



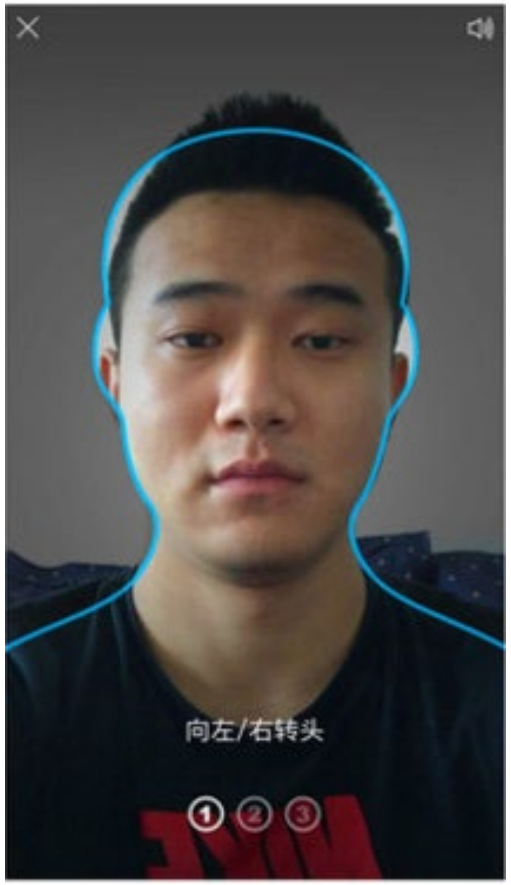
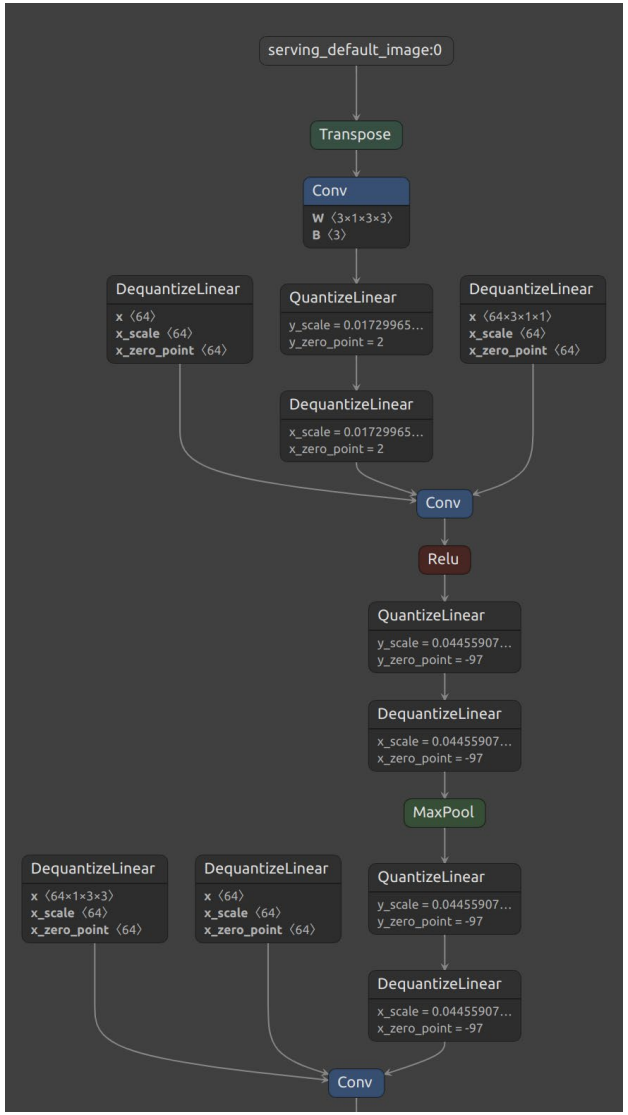
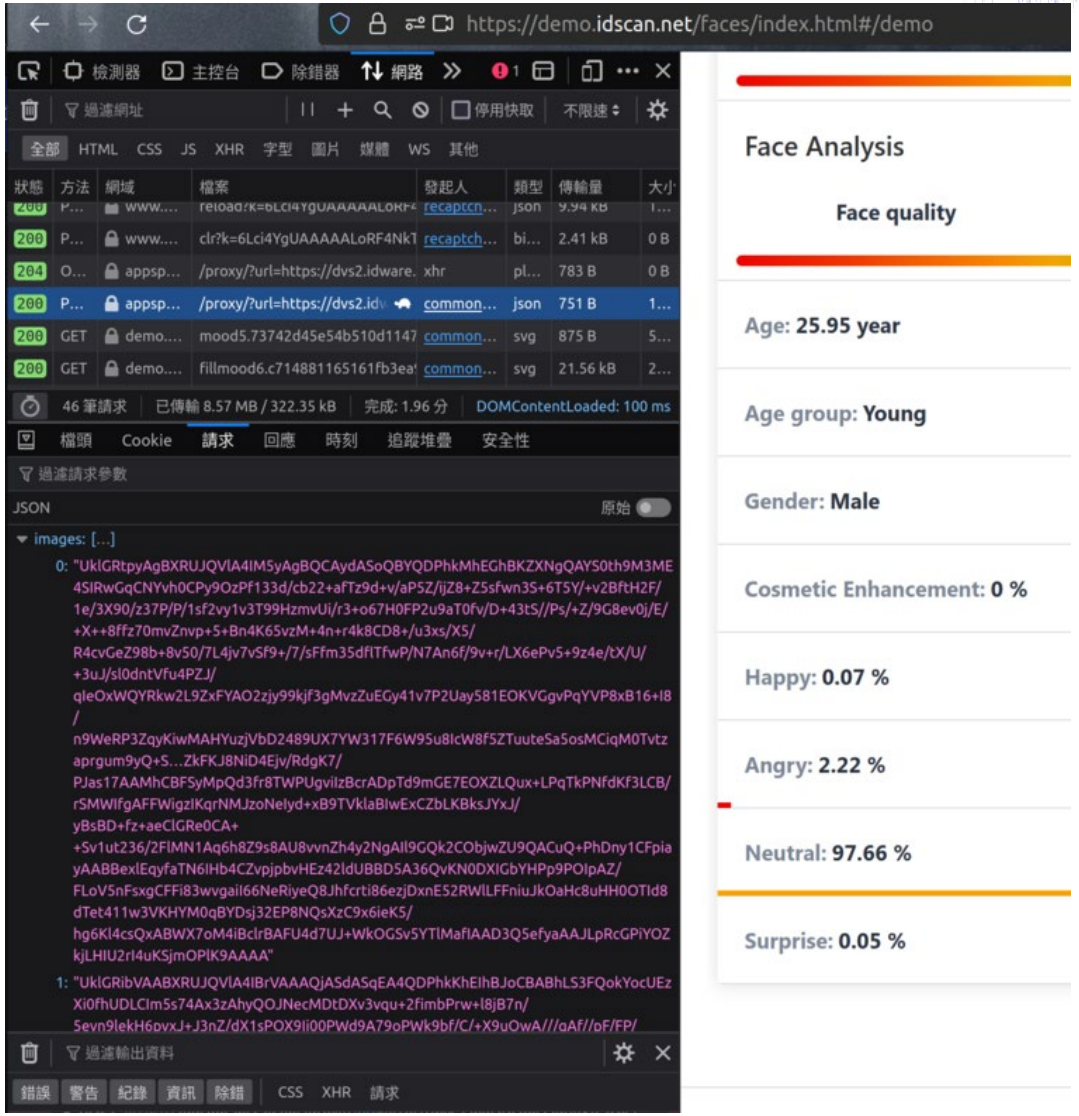


Image courtesy of https://news.cts.com.tw/cts/life/201711/201711231901178.html

- Document validity
- Security features
- Document vividness
- Facial features
- Facial vividness
- Match the features
- Done!

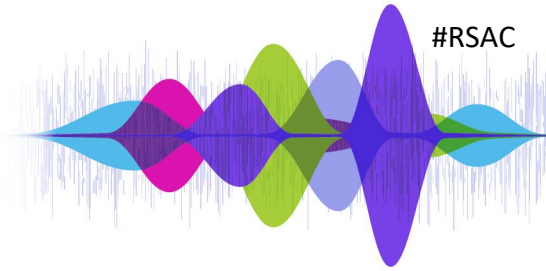
Offline models? Still to the Back-end!





RSAC 2025 Conference

Hack eKYC



Trick-Practice1800 • 9mo ago

Do you know any way to go through "video selfie" checks, I'm doing a project to prove the security of face ID verification?

1 Reply Award Share ...

mojojojo_999 • 9mo ago

Yeah, use deepfake and android virtual camera

1 Reply Award Share ...

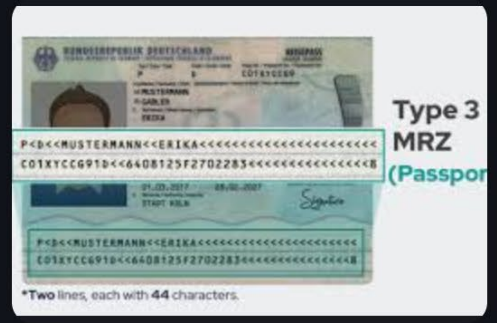
Machine readable zone | Flutter | Readable passport | Python | Passport numbers | Middle name | Scanner | Ocr | Check digit

ARATEK
What is a Machine Readable Zone (…

DESKO GmbH
Visual Inspection Zone | DESKO Gm…

LinkedIn
Machine Readable Zone (MRZ…

GdPicture
MRZ OCR SDK: ID Card, Driver …



ARATEK
What is a Machine Readable Zone (…

YouTube
IDVisor Sm…

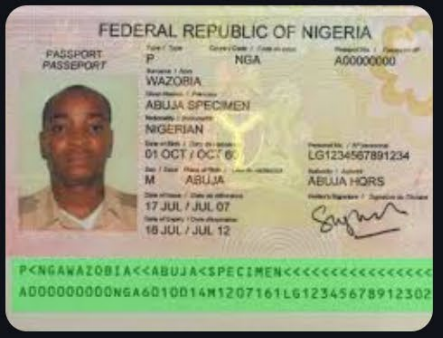
Regula Forensics
Machine-Readable Zone: Its Role in ID Verification

Xama Technologies
Passport numbers & AML checks - Xama…

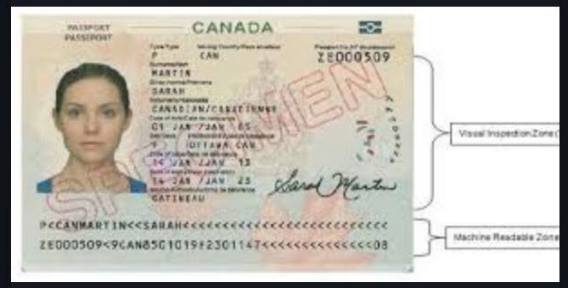
Dynamsoft
Scan Machine Readable Zone (MRZ) On …

ARATEK
What is a Machine Readable Zone (MRZ) …

Doubango
MRZ formats — ulti…

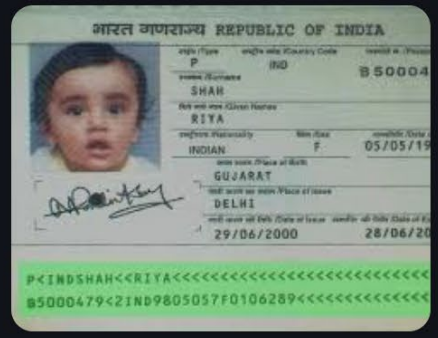


TrustDocHub
ID – Nigerian Passport MRZ Tap…



Medium
Passport MRZ reading with Tesseract.js OC…

Dynamsoft
Build a Synthetic MRZ Images Da…



TrustDocHub
ID - Indian Passport MRZ Band …

DESKO GmbH
Visual Inspection Zone | DESKO GmbH

AI models on GitHub

the Deepfake Offensive Toolkit

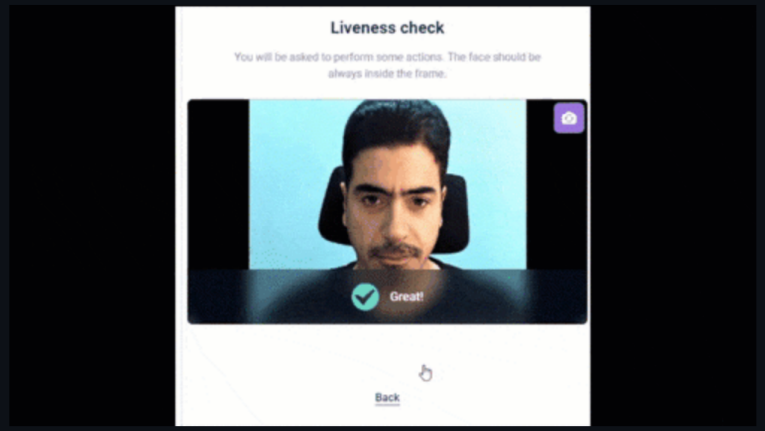
Stars 4.3k | License BSD 3-Clause | python 3.8 | build-dot passing | code-check passing

Open in Colab

dot (aka Deepfake Offensive Toolkit) makes real-time, controllable deepfakes ready for virtual cameras injection. is created for performing penetration testing against e.g. identity verification and video conferencing systems, for use by security analysts, Red Team members, and biometrics researchers.

If you want to learn more about *dot* is used for penetration tests with deepfakes in the industry, read these articles The Verge and Biometric Update.

dot *is developed for research and demonstration purposes. As an end user, you have the responsibility to obey a applicable laws when using this program. Authors and contributing developers assume no liability and are not responsible for any misuse or damage caused by the use of this program.*



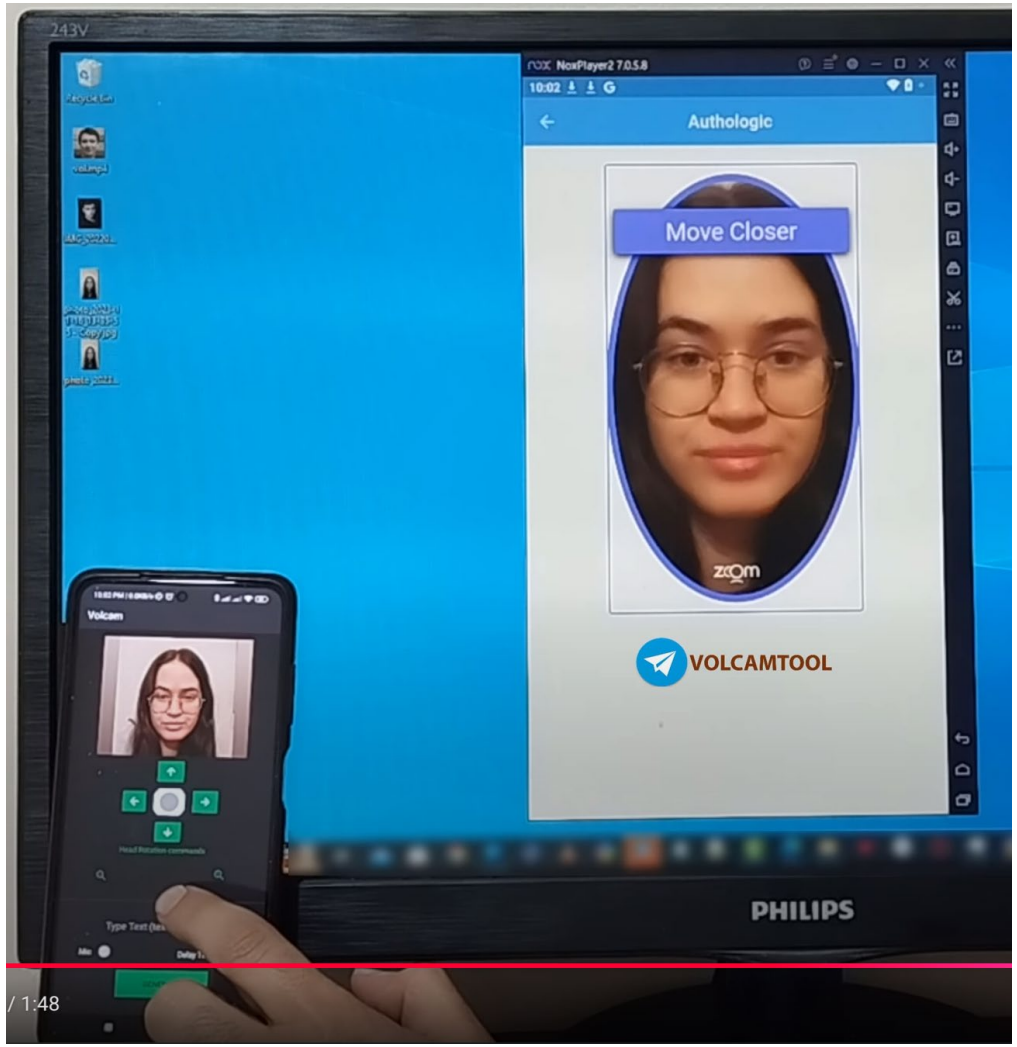
DEEPLIVECAM
REALTIME DEEPFAKE

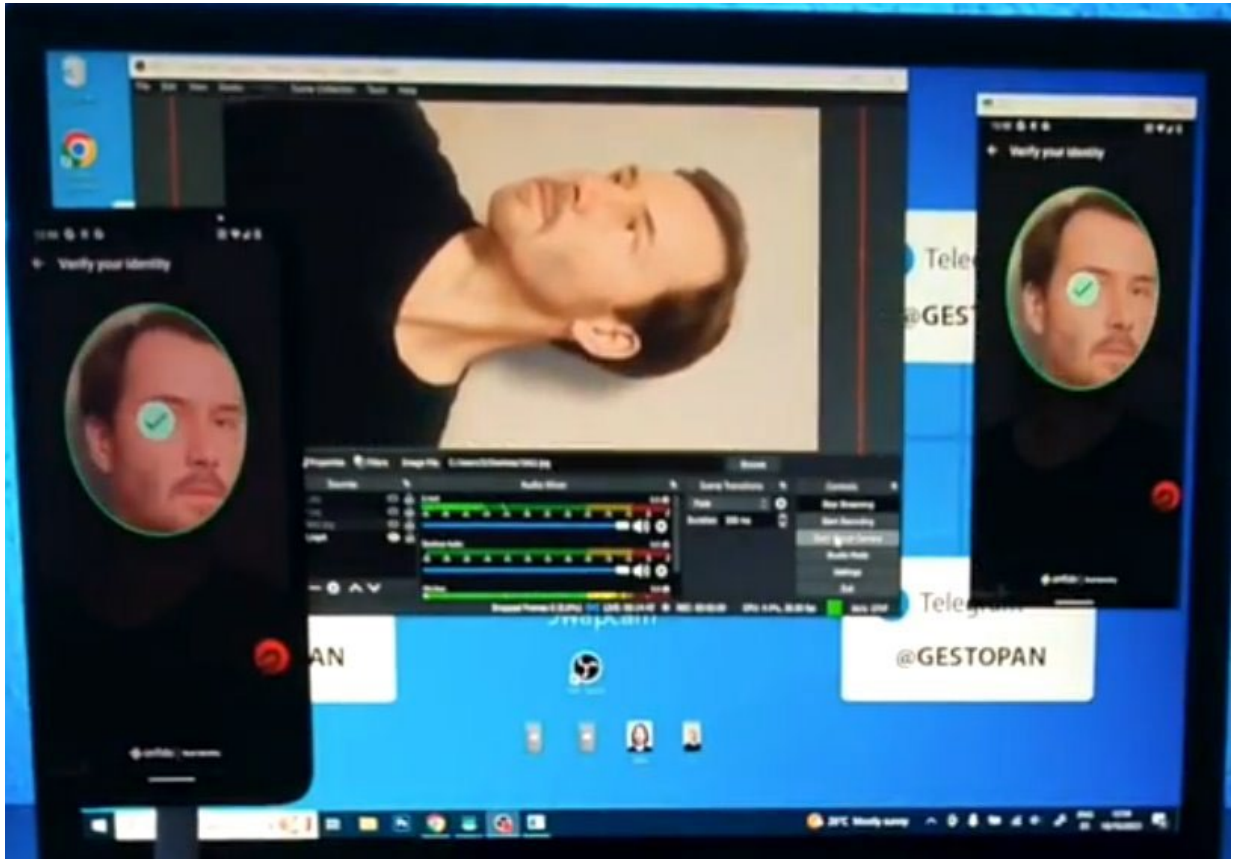
HOME | BLOG | OFFICIAL GITHUB LINK | QUICKSTART (GUMROAD) | DONATE

Home

Courtesy of Sensity AI and DeepLiveCam <3

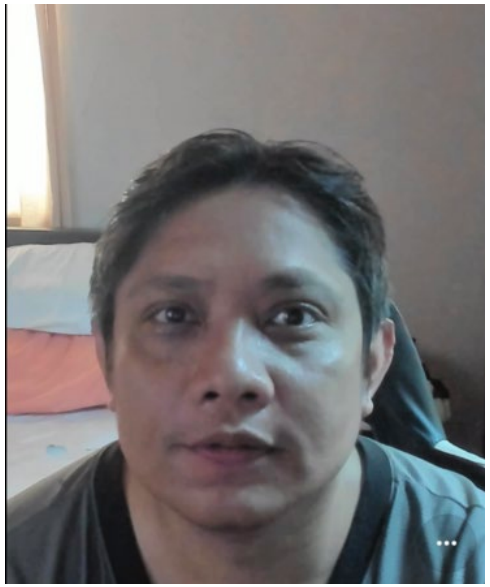
Suspicious tools in UG





Screenshot from Gestopan's YouTube channel.
Later someone complained that this is a scam.

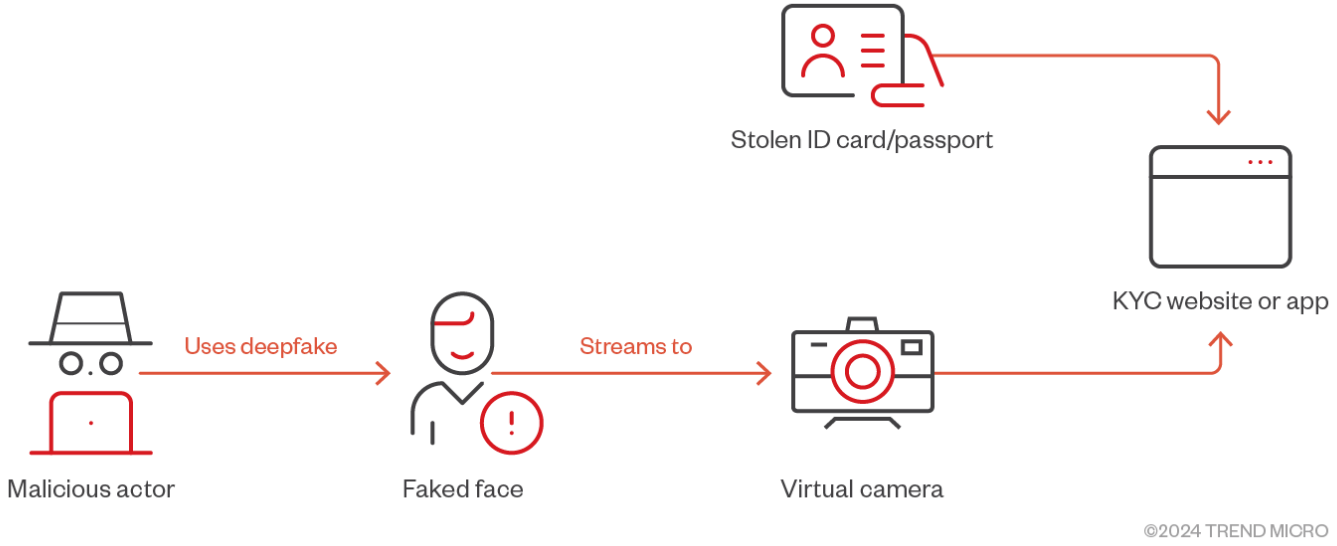
How deepfake models work?



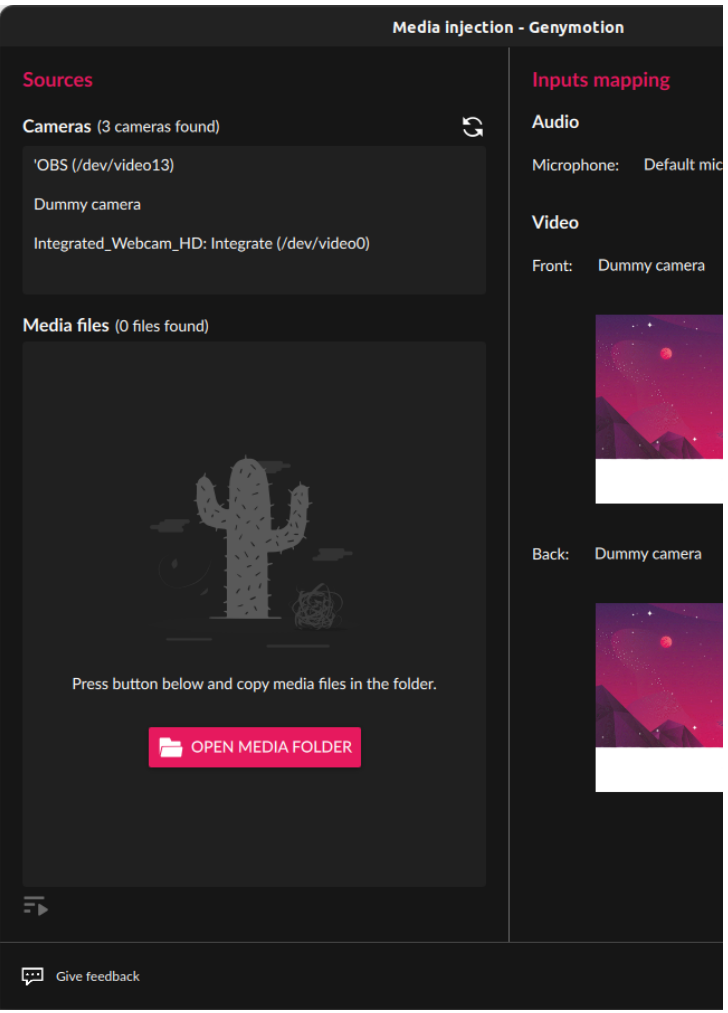
+

=

Deepfake it!


Stolen ID card/passport
KYC website or app
Uses deepfake
Streams to
Malicious actor
Faked face
Virtual camera
©2024 TREND MICRO

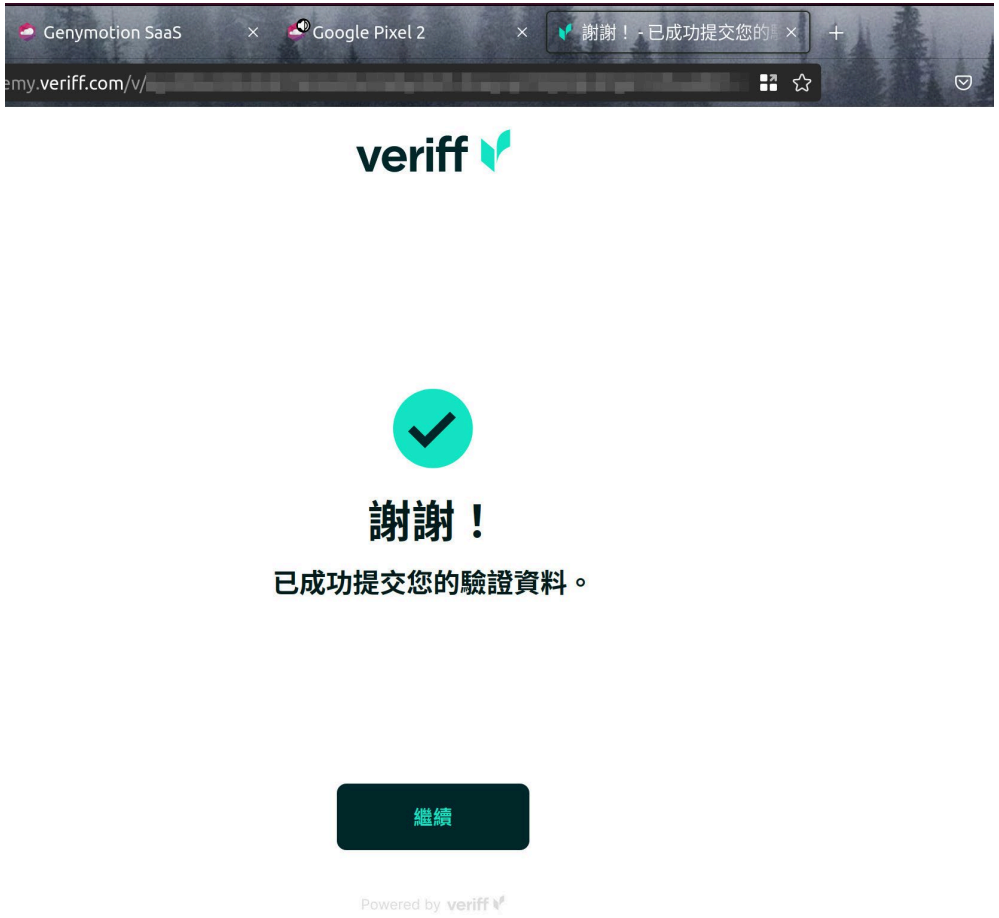
Cloud service or local?



Courtesy of https://m.thepaper.cn/newsDetail_forward_18693124

OBS + DOT + V4L
+ Android Studio
or
+ Genymotion

PhotoID + Deepfake = Bypassed!



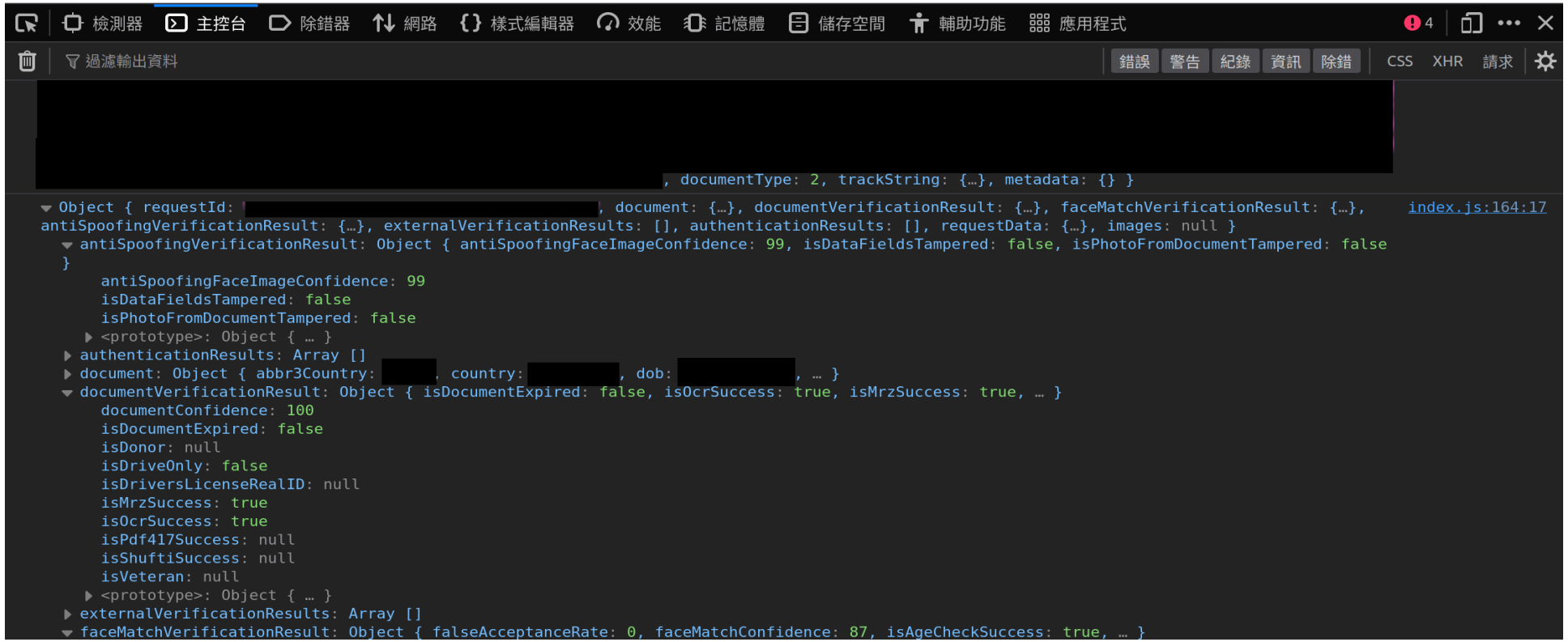
Passport

[redacted] Step 1

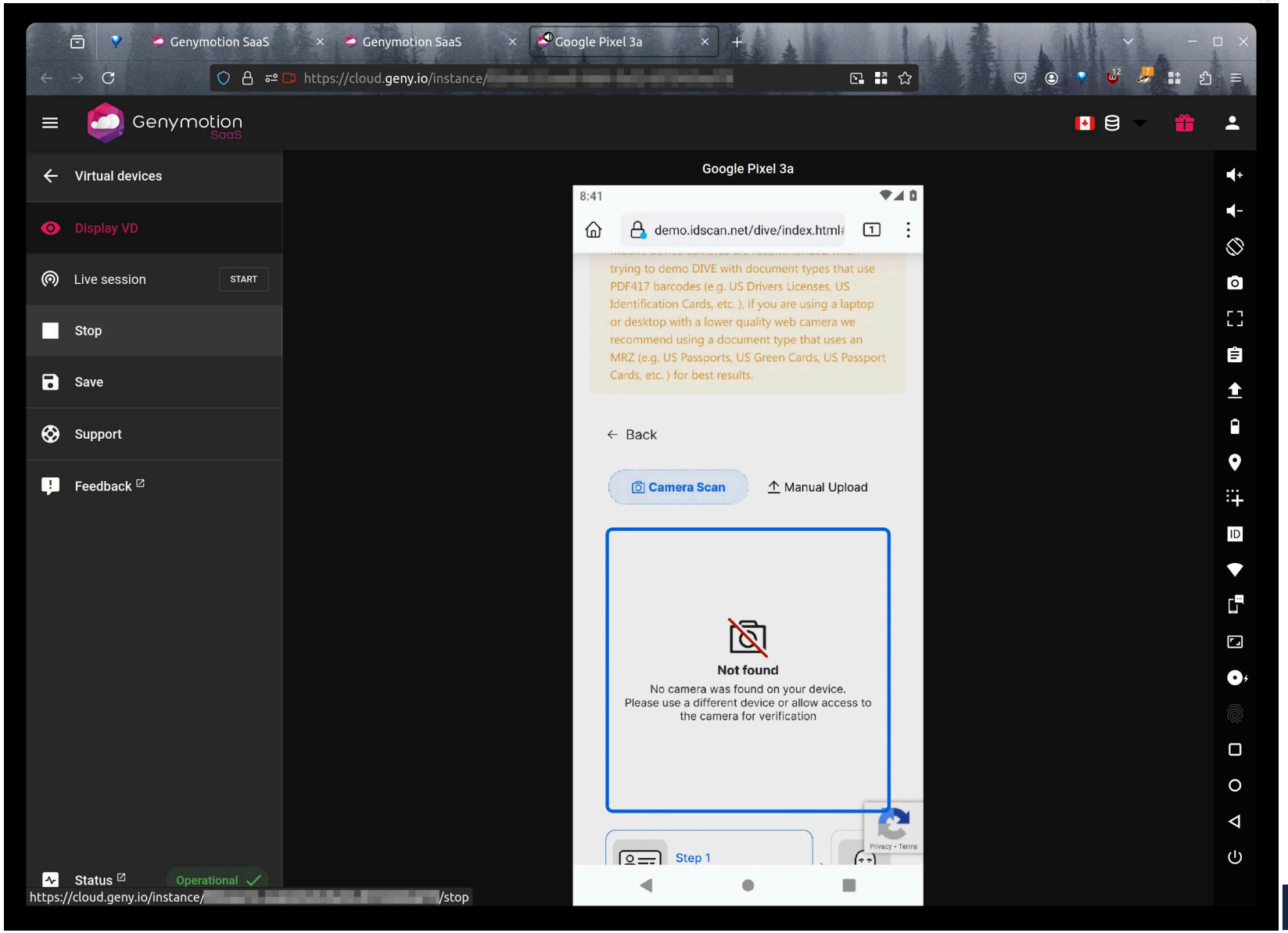
Passport Front

[redacted] Step 2

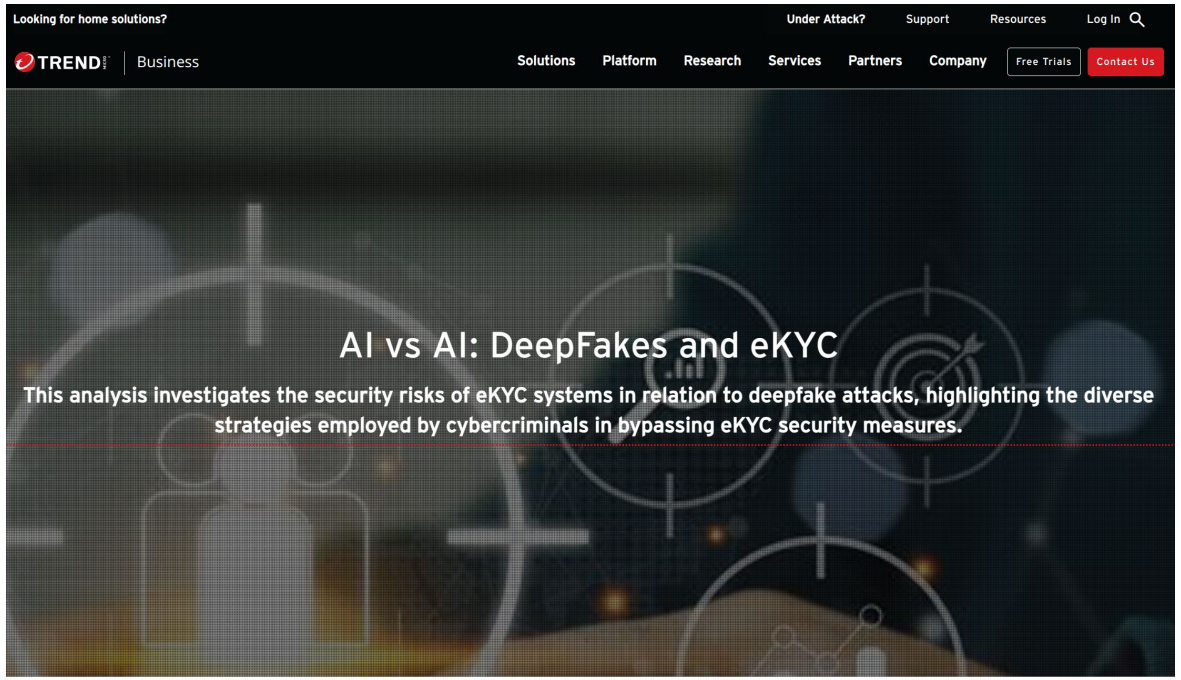
Face


檢測器 主控台 除錯器 網路 樣式編輯器 效能 記憶體 儲存空間 輔助功能 應用程式
過濾輸出資料
錯誤 警告 紀錄 資訊 除錯 CSS XHR 請求
[redacted], documentType: 2, trackString: {…}, metadata: {} }
Object { requestId: [redacted], document: {…}, documentVerificationResult: {…}, faceMatchVerificationResult: {…}, index.js:164:17
antiSpoofingVerificationResult: {…}, externalVerificationResults: [], authenticationResults: [], requestData: {…}, images: null }
antiSpoofingVerificationResult: Object { antiSpoofingFaceImageConfidence: 99, isDataFieldsTampered: false, isPhotoFromDocumentTampered: false
}
antiSpoofingFaceImageConfidence: 99
isDataFieldsTampered: false
isPhotoFromDocumentTampered: false
<prototype>: Object { … }
authenticationResults: Array []
document: Object { abbr3Country: [redacted], country: [redacted], dob: [redacted], … }
documentVerificationResult: Object { isDocumentExpired: false, isOcrSuccess: true, isMrzSuccess: true, … }
documentConfidence: 100
isDocumentExpired: false
isDonor: null
isDriveOnly: false
isDriversLicenseRealID: null
isMrzSuccess: true
isOcrSuccess: true
isPdf417Success: null
isShuftiSuccess: null
isVeteran: null
<prototype>: Object { … }
externalVerificationResults: Array []
faceMatchVerificationResult: Object { falseAcceptanceRate: 0, faceMatchConfidence: 87, isAgeCheckSuccess: true, … }

Vendors who block virtual webcam


Genymotion SaaS
Genymotion SaaS
Google Pixel 3a
https://cloud.geny.io/instance/
Genymotion SaaS
Virtual devices
Display VD
Live session
START
Stop
Save
Support
Feedback
Status
Operational
https://cloud.geny.io/instance/ /stop
Google Pixel 3a
8:41
demo.idscan.net/dive/index.html
trying to demo DIVE with document types that use PDF417 barcodes (e.g. US Drivers Licenses, US Identification Cards, etc.), if you are using a laptop or desktop with a lower quality web camera we recommend using a document type that uses an MRZ (e.g. US Passports, US Green Cards, US Passport Cards, etc.) for best results.
Back
Camera Scan
Manual Upload
Not found
No camera was found on your device.
Please use a different device or allow access to the camera for verification
Step 1

Vendors who fixed it



November 28, 2024

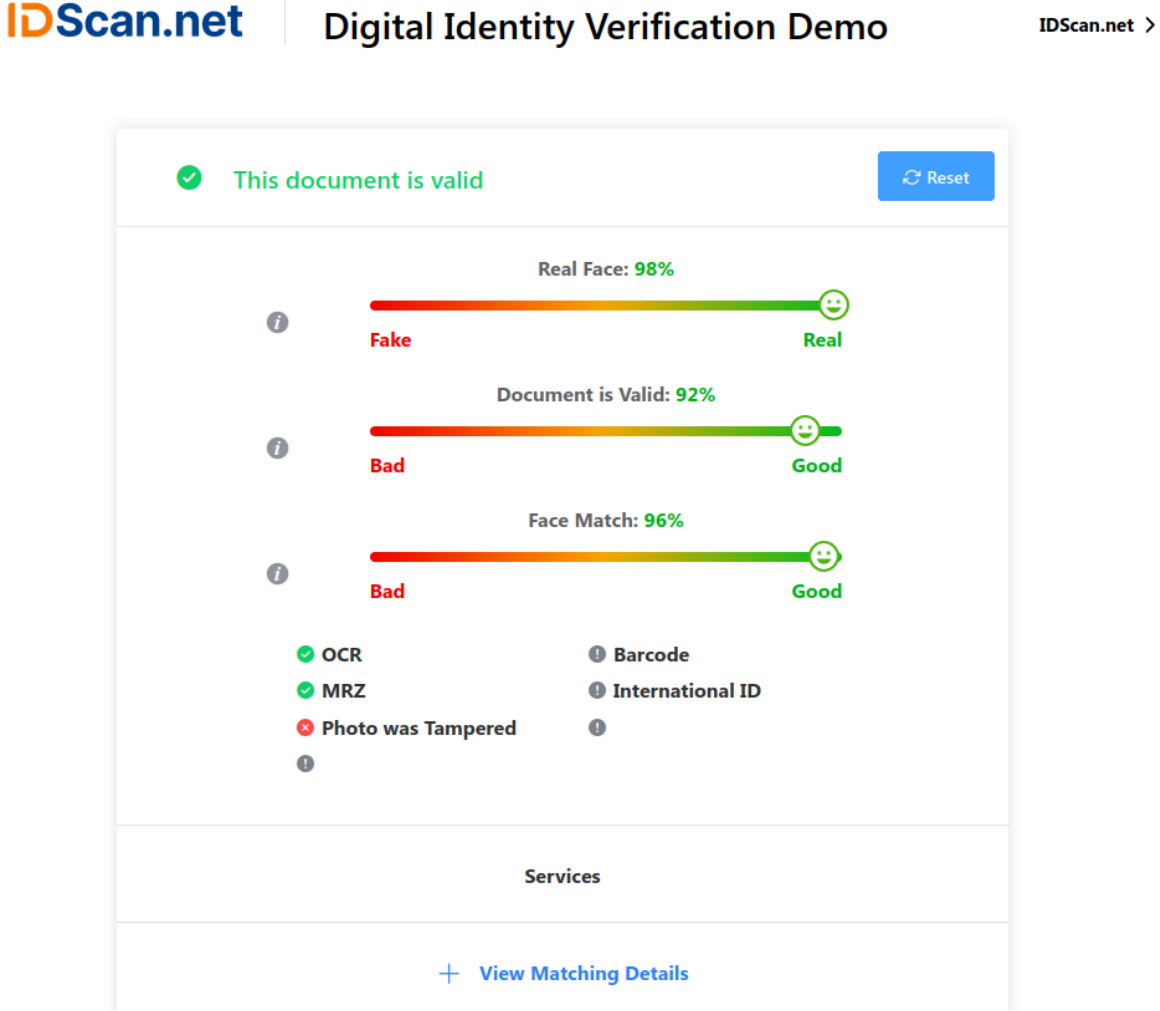
By Philippe Lin, Fernando Mercês, Roel Reyes, and Ryan Flores

With help from Vincenzo Ciancaglini, Bakuei Matsukawa, Fyodor Yarochkin, Vladimir Kropotov, and Sean Park

Know Your Customer (KYC) is a critical process — first employed by financial organizations and then adopted by other industries — that is used to verify the identity of clients, along with their financial knowledge, risks, and investment profiles. It is a mandatory regulatory process which is applied when a person opens a banking account and is designed to prevent fraud and money laundering. Today, a variety of organizations, including banks, lenders, gambling websites, cryptocurrency exchanges, and even smaller businesses such as online alcohol vendors, are increasingly adopting electronic KYC (eKYC) for online customer identity verification. The Covid-19 pandemic further boosted its adoption rate as a standard protocol for online customer

Related Posts

- AI in the Crosshairs: Understanding and Detecting Attacks on AWS AI Services with Trend Vision One™
- AI Assistants in the Future: Security Concerns and Risk Management
- Silent Sabotage: Weaponizing AI Models in Exposed Containers
- The Easy Way In/Out: Securing The Artificial Future
- Generative AI in Elections: Beyond

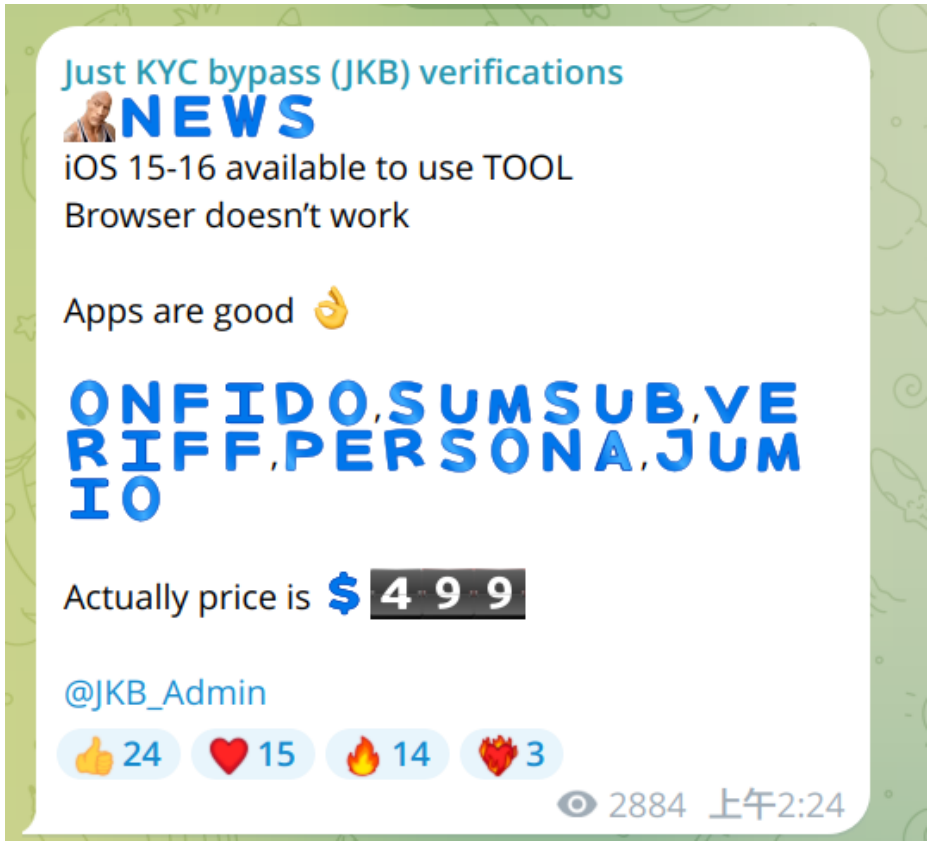


RSAC 2025 Conference

Problems!

Many Voices.
One Community.

Bypass one ?= Bypass all

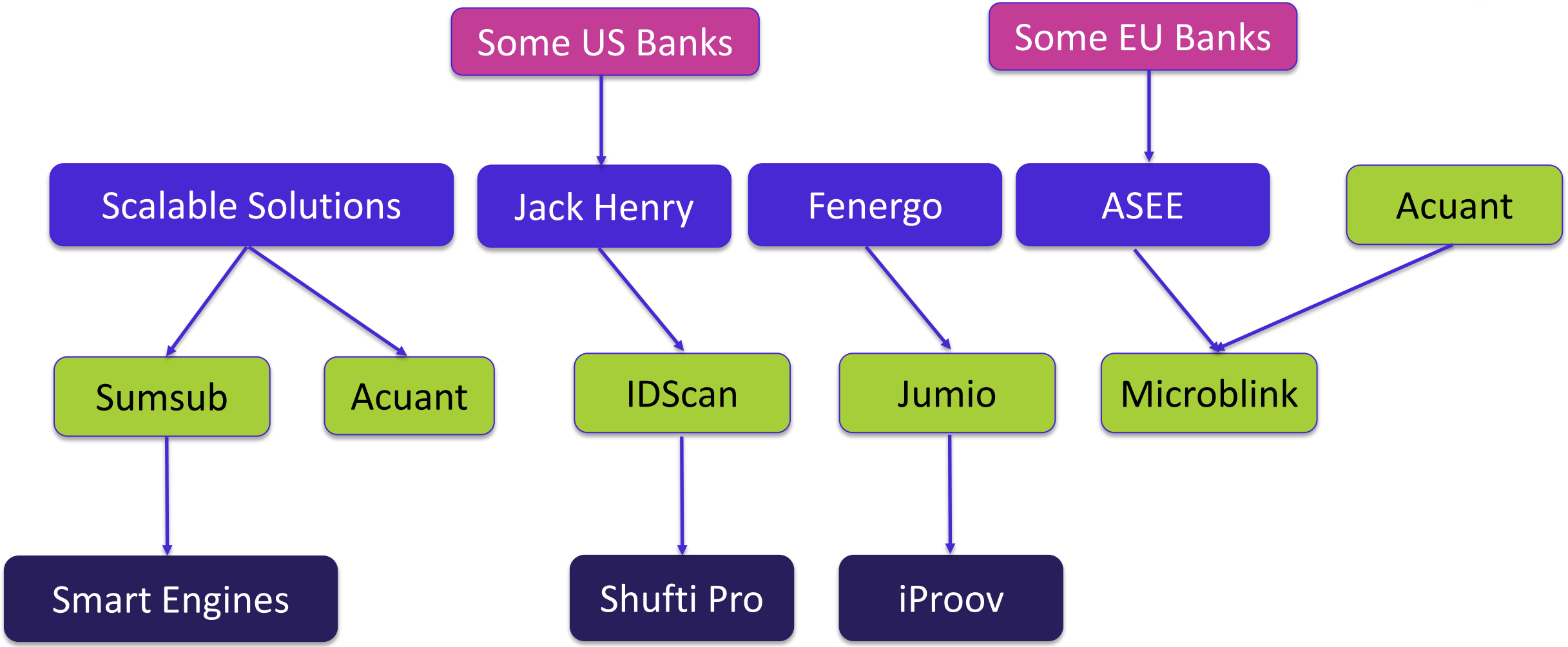


Mhis There(kyc all revise) Reply

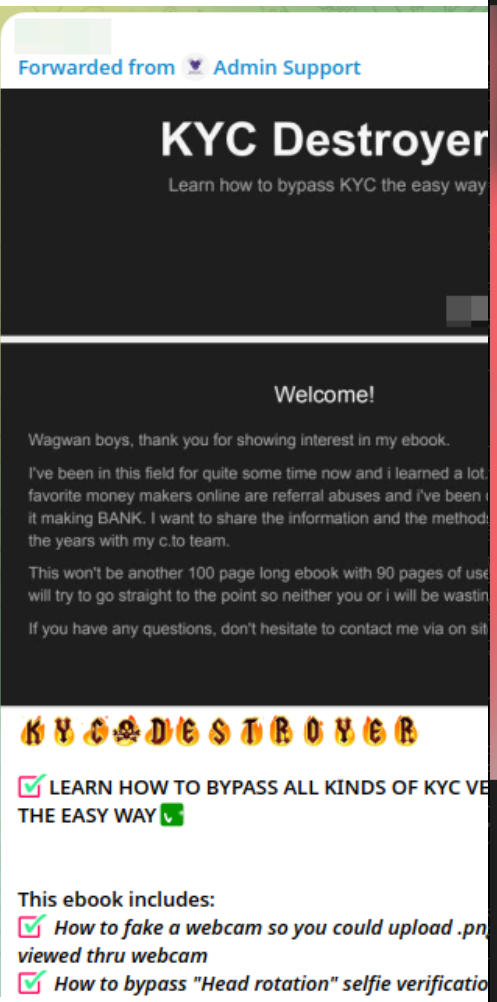
Wts (Sell) Ready accounts or Kyc Service
SELL SELL SELL
Ready Made or Kyc service

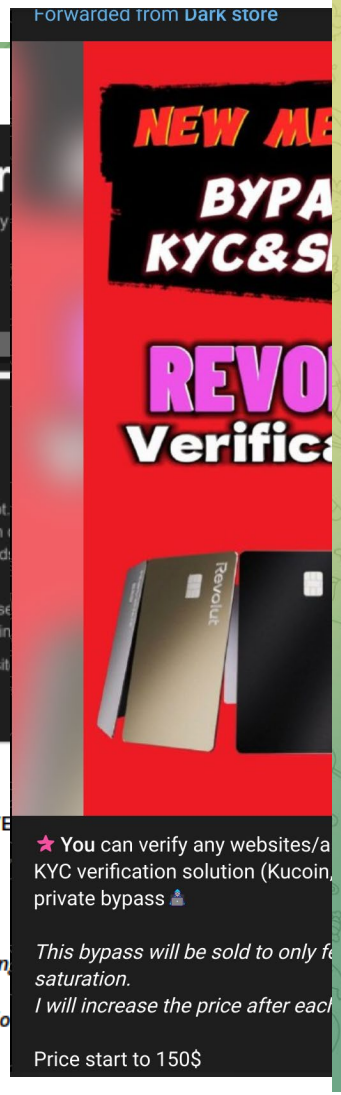
Freecash 8-10
Okx 8-10$
Singtel 25$
Wise 20$.
Coinlist 15$.
Binance 10-12
Alipay 25$
Bybit 8-10$
Galxe 8-10$
Kucoin 8-10$
Backpack 8-10
Bitget 8-10
BingX 8-10
Coinbase 8-10 FOR GITCOIN
Coinstore 6-8$
Mexc 8-10
Haskey Global 8$
Civic 5$
Whitebit 7-8$
Faceit 7-8
Jeton Wallet 20$
Avito 15$
Parpeck money 20$
Gate oi 8-10 $
Holonym 7-8$
Stake lvl 3/4 15-30$
Kyc Telegram 8-10
Moonpay 15$
Xapo bank 80-100$
Worldremit 8-10$

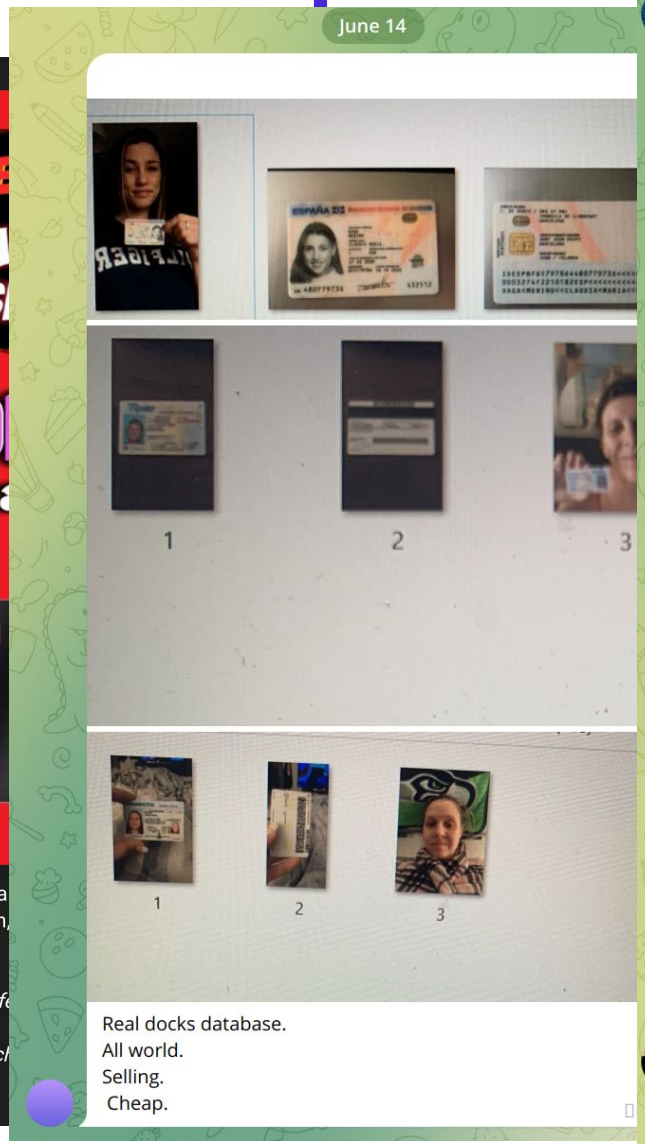
Estimate the supply-chain

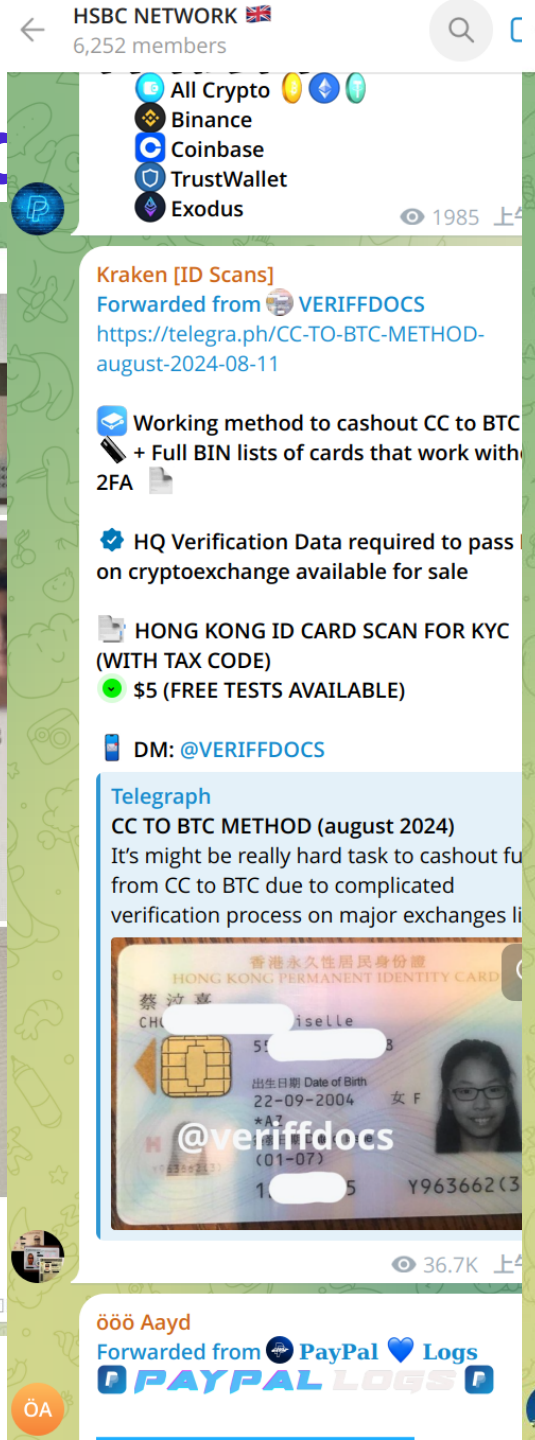


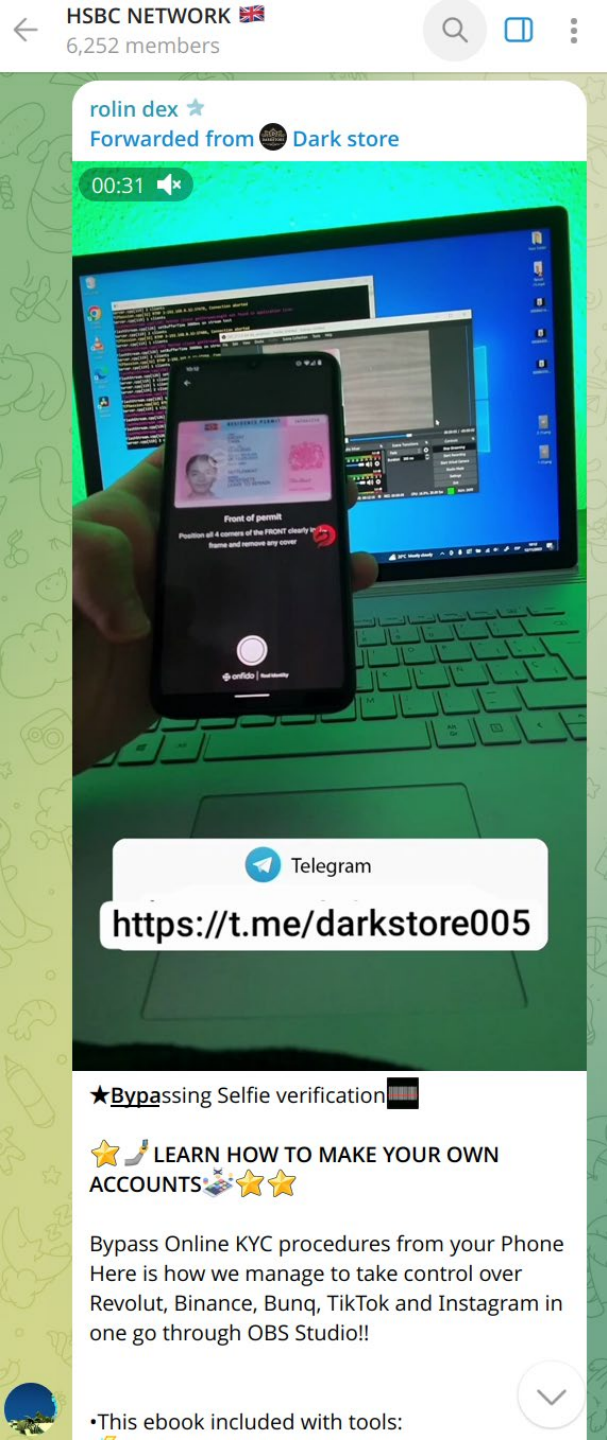
Criminals are one-step ahead


Forwarded from Admin Support
KYC Destroyer
Learn how to bypass KYC the easy way
Welcome!
Wagwan boys, thank you for showing interest in my ebook.
I've been in this field for quite some time now and i learned a lot.
favorite money makers online are referral abuses and i've been
it making BANK. I want to share the information and the method
the years with my c.to team.
This won't be another 100 page long ebook with 90 pages of use
will try to go straight to the point so neither you or i will be wastin
If you have any questions, don't hesitate to contact me via on sit
KYC DESTROYER
LEARN HOW TO BYPASS ALL KINDS OF KYC VE
THE EASY WAY
This ebook includes:
How to fake a webcam so you could upload .pn
viewed thru webcam
How to bypass "Head rotation" selfie verificatio








HSBC NETWORK
6,252 members
rolin dex
Forwarded from Dark store
00:31
Telegram
https://t.me/darkstore005
★Bypassing Selfie verification
LEARN HOW TO MAKE YOUR OWN ACCOUNTS
Bypass Online KYC procedures from your Phone
Here is how we manage to take control over Revolut, Binance, Bunq, TikTok and Instagram in one go through OBS Studio!!
•This ebook included with tools:

Criminals are one-step ahea

KYC Bypass Method

Updates:

1.VcamPro App alternative Is Now Incl
Method, To Bypass KYC From The Pho
The Phone Camera)

2. +15000 Documents Pack (Front, Bac
Offered For My Clients For a Good Pric
Per Doc, and for 1k For Others

3. All The Links In The Method Are Upc

4. More Videos added To Make The Pr

5. Price Updated To 800 Usdt.

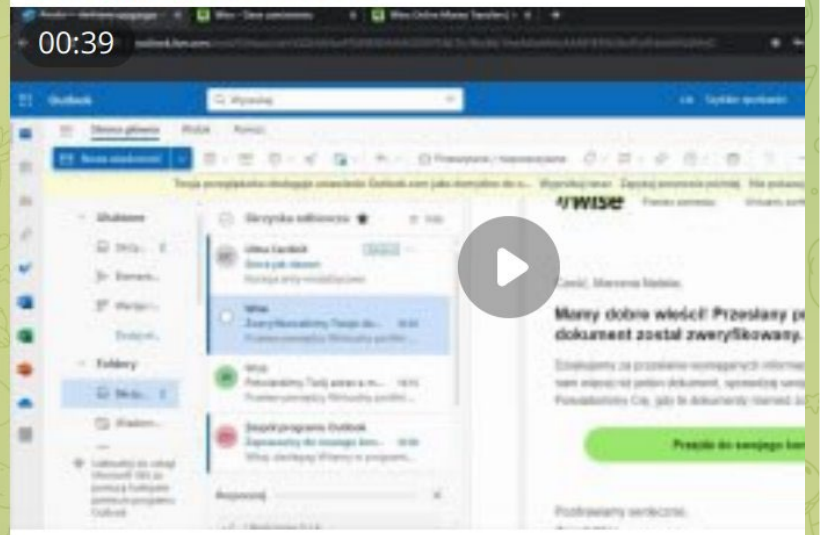
Dm: @FluxFury

Welcome.

14 1

1418 Flux

STYX PRIVATE SECTION



Detailed KYC bypass for Wise (USA/Europe). Set up
machine and browser to work on KYC bypass. Full video
information is already available in the Styx Private Secti
the pinned message)

**Детальное прохождение верификации KYC Wis
(USA/Europe).** Настройка машины и браузера для ра
обходу KYC. Полное видео и вся информация уже до
Приватной Секции Styx (Условия в закреплённом со

Telegram support: @AlexaSTYX3

9555 ed

KYC Bypass Method

Product Page Updated With The Newest Version + The VcamPro App

Purchase Directly From My Shop

https://fluxfury.mysellix.io/product/fluxfury-kyc-bypass-method-high-quaity-method-to-bypass-high-security-kyc-systems

Read The Description There

For Any Questions

Dm: @FluxFury

fluxfury.mysellix.io

FluxFury KYC Bypass Method | High Quaity Method To Bypass High Security KYC Syste...

Check out FluxFury KYC Bypass Method | High Quaity Method To Bypass High Securit...

11

1444 Flux Fury, 下午3:04

BULLSNIDER SERVICE
1,468 subscribers

Pinned message
Master Phone-Based Verification Training (...

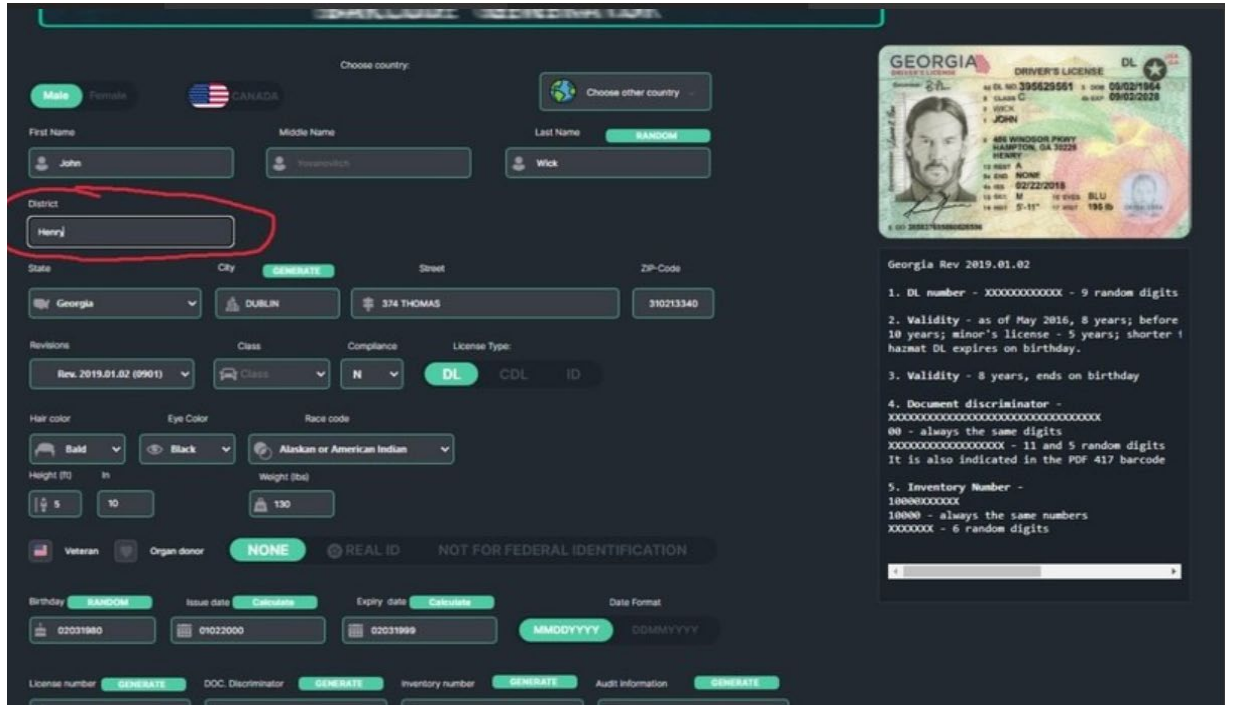
Revolut Liveness Bypass on PC Monitor

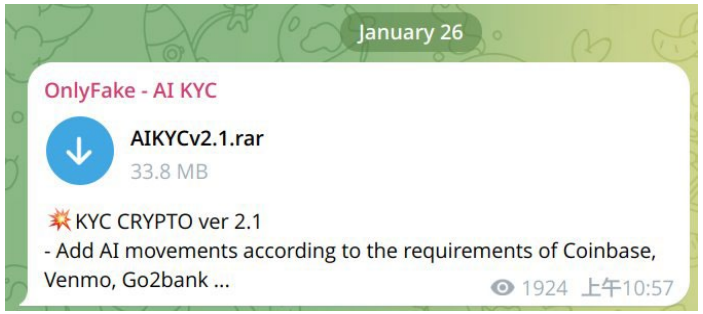
Fully Functional After the September 2024 Security Update

Compatible with:
- SumSub
- Jumio
- Onfido
- And other KYC systems

Price: $3000 USD

Photo ID generators




January 26
OnlyFake - AI KYC
AIKYCv2.1.rar
33.8 MB
KYC CRYPTO ver 2.1
- Add AI movements according to the requirements of Coinbase, Venmo, Go2bank ...
1924 上午10:57

Bypass KY

#RSAC

Mose

Верификация Skrill - 55$ [СНГ]
Верификация Neteller - 55$ [СНГ]
Верификация Wise - 80$ [EU]
Верификация Huobi - 40$ [СНГ]
Верификация OKX - 60$ [EU]
Верификация KuCoin - 60$ [EU]
Верификация WhiteBit- 60$ [EU]
Верификация OkCoin - 60$ [EU]
Верификация Mexc -60$ [EU]
Верификация ZeusX - 50$ [EU]
Верификация Binance - 40$ [СНГ]
Верификация AstroProxy- 25$ [СНГ]
Верификация Iproyal- 25$ [UA]
Верификация G2G - 25$ [СНГ]
Верификация Igvault - 17$ [EU]
Верификация Bybit - 10$ [СНГ]
Верификация вашего аккаунта Bitzlato

Это не весь список который мы делаем
Если нету в списке нужной вашей вери
ЛС
Также делаем верификацию и вашего а
готового аккаунта
TG - @pozzitifvv

Rubix_support
USA 🇺🇸 - если актуально, запрашивайте отдельно. Список большой.
(If relevant, request separately. The list is large.)

RuBiX🎲 Check my bio, [20.08.2023 23:56]
🇺🇿 Zoomrad Bank - 280$
🇺🇿 Ipak Yo'li Bank - 250$
🇺🇿 Anorbank - 250$
🇺🇿 Agrobank - 250$
🇺🇿 Asaka bank 260$
🇺🇿 Capital Bank - 490$
🇺🇿 Davr bank - 250$
🇺🇿 NBU - 250$ (VISA PLATINUM): 399$
🇺🇿 Tenge bank - 250$

🔥🇺🇿 Биржа - От 130$
(в связке с банком)
🔥🇺🇿 Esim (Билайн, Уселл) - 45$ (от 5 шт)

🌎⬇️🌎

🇰🇿 Forte Bank: 280$
🇰🇿 Altyn Bank: 260$
🇰🇿 Smart Bank: 260$
🇰🇿 Simply: 220$
🇰🇿 Tayyab: 220$
🇰🇿 RBK: 260$
🇰🇿 BCC: 260$

🇰🇿 Binance: 130$ в связке ∞

🇰🇿 Esim: 50$

✅✅✅КОНТАКТ - @RuBiX24_Support
449 上午11:03

December 29, 2023

Rubix_support
$ PriceList $

Lydia 🇫🇷: 299$
Bitsa 🇪🇸:270$
Bbva 🇪🇸: 580$
Pyypl 🇪🇬 :250$
WU+ 🇦🇹 349$ // 💳 ± 599 $
Bankaustria 🇦🇹: 490$
Wise 🇪🇺: 280$ с депозитом // 💳 ± 390$
Wise 🇬🇧 🇺🇸: 349$
Cryptopay 🇪🇺 🇬🇧: 250$
Revolut 🇪🇺: 289$
Revolut 🇬🇧: 450$
Revolut 🇺🇸: 450$
Dukascopy: 🇪🇺 299$
Tally 🇬🇧 250$
Suits ME 🇬🇧 + 💳 : 399$
Icard 🇧🇬 : 270$
Binance: 🇪🇺 199$ // 💳 ± 369 $
Wirex 🇬🇧 🇮🇪 : 249$
Weststein: 🇪🇺 199$
W1tty: 🇪🇺 199$
AdvCash 🇪🇺: 260$ // 💳 ± 369 $
Blackcatcard 🇲🇹 : 220$ // 💳 ±369 $
Zen com 🇪🇺: 280$ // 💳 ± 369 $ (E-SIM)
Crypterium: 🇪🇺 220$
Skrill 🇪🇺: 199$
Yopay 🇪🇺 : 199$
Dzing 🇬🇧: 270$
Bunq 🇩🇪 🇪🇸 🇬🇧 🇪🇺 : 370$
PayPall 🇪🇺: 199$
Sumsub 🇪🇺: 199$
Astropay 🇪🇺: 250$
Paysera 🇪🇺: 270$
Bankera 🇪🇺 3 LVL :299$
Coinpayments 🇪🇺: 199$
Paysend 🇪🇺: 250$
Mercuryo 🇪🇺: 199$
Mode 🇪🇺: 199$
Genome 🇬🇧:220$
Vialet 🇬🇧:250$
Curve: 🇬🇧199$
Akt io: 🇪🇺 220$
Eglobex black: 🇪🇺250$
Omniwire: 🇪🇺250$
Nagapay 🇪🇺 🇬🇧 199$
Bilderlings 🇪🇺 🇬🇧 250$
Guavapay 🇬🇧 250$
Frost 🇬🇧 259$
Bank Austria 🇦🇹 450$
Payoneer 🇪🇺199$
Биржи / Exchange: 🇪🇺 🇬🇧 🇺🇸 170-190

✅✅✅КОНТАКТ - @RuBiX24_Support
403 edited 上午11:03

February 6

KYC Services

Personal Bank accounts

Price updating !

Bunq - $250 (Netherland | France | Spain)
Revolut - $250 (France | Italy | UK | Germany)
Zen - $199 (Netherlands | Croatia)
Wise - $149 (Usa | Uk | France | Italy)
Stripe - $249 (Usa | Uk)
Paypal - $79 (Usa | Uk | Germany | Italy)
Payoneer - $149 (Usa)
N26 - $350 (Germany)
Vivid - $300 (Germany | Spain)
Icard - $199
Chase - $149 (Uk | Usa)
Cashapp BTC Enabled - $199
Bankera - $200

Autobuy -> KYC Legion Store

Support - @Kyclegion
473 edited 下午5:51

TREND MICRO
RSAC 2025 Conference

Photo and PhotoID stored on servers

Signzy investigating KYC customer data breach

Dec 6, 2024, 12:26 pm EST | Chris Burt

Alleged Data Breach in Transak's KYC Database

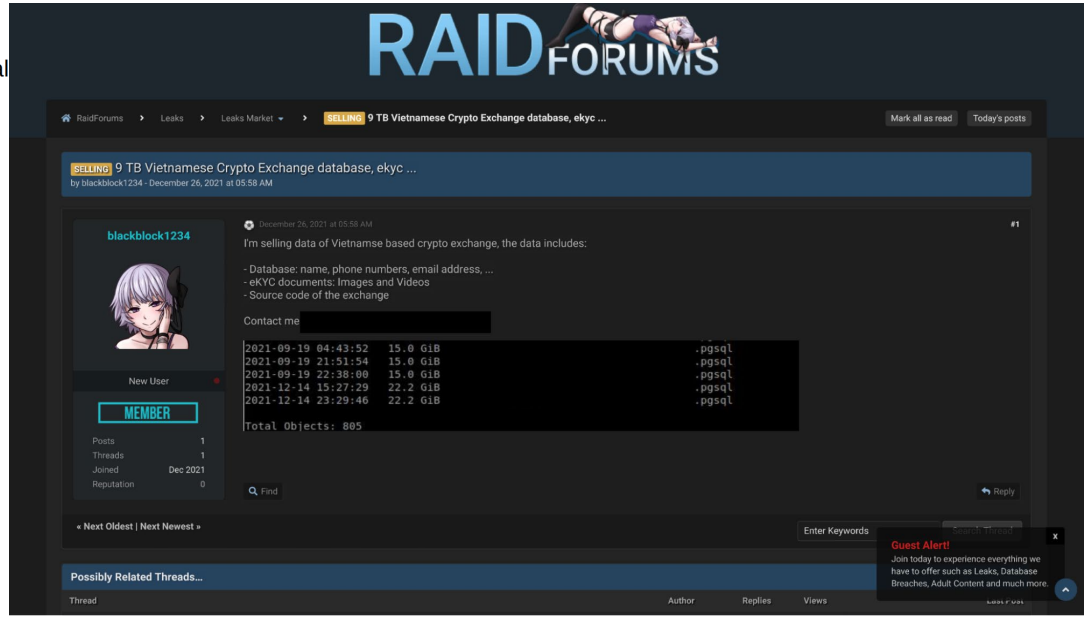
BY ANUPRIYA / FEBRUARY 4, 2025 / CYBER SECURITY NEWSCYBERSECURITYDATA BREACH

The Register

Cybercriminals threaten to leak all 5 million records from stolen database of high-risk individuals

It's the second time the World-Check list has fal

Connor Jones


RAID FORUMS
RaidForums › Leaks › Leaks Market › SELLING 9 TB Vietnamese Crypto Exchange database, ekyc ...
Mark all as read
Today's posts
SELLING 9 TB Vietnamese Crypto Exchange database, ekyc ...
by blackblock1234 - December 26, 2021 at 05:58 AM
blackblock1234
New User
MEMBER
Posts 1
Threads 1
Joined Dec 2021
Reputation 0
December 26, 2021 at 05:58 AM
#1
I'm selling data of Vietnamese based crypto exchange, the data includes:
- Database: name, phone numbers, email address, ...
- eKYC documents: Images and Videos
- Source code of the exchange
Contact me
2021-09-19 04:43:52 15.0 GiB .pgsql
2021-09-19 21:51:54 15.0 GiB .pgsql
2021-09-19 22:38:00 15.0 GiB .pgsql
2021-12-14 15:27:29 22.2 GiB .pgsql
2021-12-14 23:29:46 22.2 GiB .pgsql
Total Objects: 805
Find
Reply
« Next Oldest | Next Newest »
Enter Keywords
Guest Alert!
Join today to experience everything we have to offer such as Leaks, Database Breaches, Adult Content and much more.
Possibly Related Threads...
Thread
Author
Replies
Views

Screenshot courtesy of https://www.cadosecurity.com/blog/fallout-from-log4shell-related-vietnamese-cryptocurrency-exchange-attack-kyc-data-for-sale-on-dark-web

404

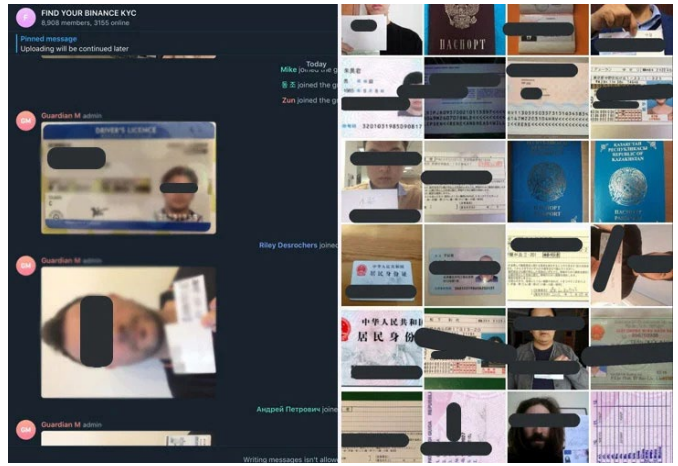
ABOUT RSS SUPPORT/FAQ PODCAST FOIA FORUM ARCHIVE

NEWS

ID Verification Service for TikTok, Uber, X Exposed Driver Licenses

JOSEPH COX · JUN 26, 2024 AT 9:39 AM

Courtesy of 404 Media



Binance KYC leak, courtesy of https://thehackernews.com/2019/08/binance-kyc-data-leak.html

TREND MICRO
RSAC 2025 Conference

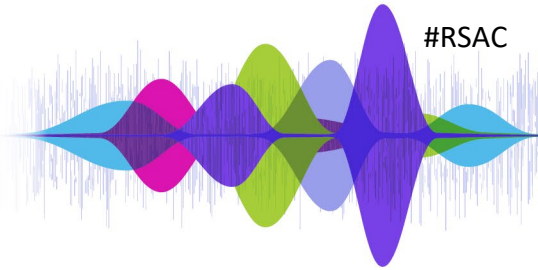
RSAC 2025 Conference

What shall we do?

Apply what you have learned today!

- End-users:
  - Think twice before you go through eKYC
  - List which PhotoID you've provided and (maybe) apply for a new one

Apply what you have learned today!



- KYC Customers:
  - Evaluate eKYC providers. Choose wisely!
  - Ask your provider how they deal with deepfakes, data leaks, attackers.
    - "Do you detect stolen photo IDs? Do you have a stolen ID database?"
    - "Do you store my customer's data? Are they encrypted?"
    - "How good is your AI model against deepfakes?"
    - "Have you hired a pentesting team to test the systems?"
  - Review your provider's tech supply-chain

Call for action

- For KYC providers:
  - Pentest your current eKYC procedure
  - Develop & Encrypt offline models
  - Share a DB of stolen ID among the industry
  - Keep testing against the latest deepfake tools
  - Monitor underground forums
  - Fingerprint user devices and user behaviors

RSAC™ 2025 Conference

Many Voices.
One Community.

philippe_z_lin@vicone.com
roel_reyes@trendmicro.com